View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by STORE - Staffordshire Online Repository

Defining a new composite cybersecurity rating scheme for SMEs in the U.K.

Andrew Rae and Asma Patel

School of Computing and Digital Technologies,
Staffordshire University,
Stoke-on-Trent, UK
r021335f@student.staffs.ac.uk & asma.patel@staffs.ac.uk

Abstract. The 5.7 million small to medium enterprises (SMEs) in the U.K. play a vital role in the national economy, contributing 51% of the private sector. However, the cyber threats for SMEs are increasing with four in ten of businesses experiencing a cyber attack in the last twelve months. One significant treatment of this growing concern is in the implementation of long-established information security standards and best-practices. Yet, most SMEs are not undergoing the certication process, even though the current threats are now widely published by the government. In this paper, we look at the disconnect of cyber threats faced by SMEs considering their current security postures and perceptions. We also identify the influencing factors needed to improve security behaviours and engagements with information security best-practices. We then propose a new foundational composite cybersecurity rating scheme aimed at SMEs. The focus of our scheme is to ascertain and measure the security behaviours, perceptions and risk propensity of each SME, as well as their technical systems. To that end, we define our 5x5 matrices based scheme by combining the measurements ascertained from the behavioural as well as technical audits. The preliminary evaluation results demonstrate that this approach provides a higher level of insight, engagement and accuracy as to an SME's individual security posture.

Keywords: Cybersecurity · Data Security · Information Security · Cyber Essentials · ISO 27001 · SMEs · Security Behaviours · Risk Propensity.

1 Introduction

In 2018, a survey done by the U.K. government revealed that four in ten U.K. businesses suffered a cyber-attack within the last twelve months, with the average cost for an SME of £1,570 per attack[13]. However, another survey [9] on the security of small business showed that less than a quarter of small businesses cited cybersecurity as one of their top concerns. There appears to be a disconnect in what SMEs, particularly smaller businesses, perceive as top risks when asked. This contradictory situation is in a time when in May 2018, the U.K. put into force the new data protection regulation [20]. This regulation now places the

onus and legal requirements on businesses to not only protect their data, but to also proactively notify the Information Commissioner's Office of any breaches or face serious financial consequences such as fines of up to 4% global turnover or €20 million .

Running in parallel with this concern is the increasing requirement within the public sector to engage SMEs and push businesses into achieving a recognised cyber or information standard before being allowed into the procurement process. The U.K. Government has gone further and set a 2022 target of achieving 33% procurement of all their contracts undertaken by SMEs [8]. As this aim of the government moves forward, it produces opportunities, but it also presents significant challenges. The perception and current security postures of SMEs, especially around data and information security risks, are critical challenges. Consequently, these challenges contribute to the lack of SMEs' engagement to existing standards. Cyber Essentials [26] and ISO 27001 [21] are the two prime examples that provide the key criterion for working with the government; however, the take up of these standards is still very low since the release of Cyber Essentials in June 2014 and [21] last major update in 2015. As the U.K. Government's own Minister for Digital and Culture admitted [17], just over 0.1% of the 5.7 million SMEs in the U.K. have undertaken Cyber Essentials even though that was particularly designed to help facilitate and encourage smaller businesses to achieve a recognised standard.

This paper proposes a new robust and consumer-friendly cyber rating scheme. This scheme provides better personalised security insights of the persons reasonable for a business and how their behaviours, awareness and risk propensity impact on these insights. Following are the core principles which defines the new composite cybersecurity rating scheme:

- To provide a preliminary outline of a robust consumer-friendly cyber rating scheme which considers the technical requirements, as well as the behavioural insights of SMEs, through a new composite rating threshold-based model.
- To devise a scheme which has the capability of promoting and incentivising secure behaviours as well as helping encourage progression into recognised information security standards.
- Enable higher levels of protection and increase informed decision-making opportunities for consumers and organisations within a supply chain.

Rest of the paper is organised as follows. Section 2 illustrates related work. Section 3 outlines the proposed model design and Section 4 demonstrates the initial evaluations using expert interviews and two quantitative surveys. Section 5 concludes and presents future research workstreams.

2 Related Work

This section discusses the related work in the key research areas required to start defining a new scheme.

2.1 SME security behaviours and perceptions

When looking at the literature concerning U.K. SME security behaviours and perceptions, the options are quite limited. [18] identified some attitudinal changes needed within SMEs to increase the uptake in existing security standards. The big hypothesis put forward is that SMEs choose not to spend on information security as they believe the risks are acceptable and, therefore, do not see the benefits of investing in this area. This suggests that SMEs need clear, short-term and measurable benefits or incentives to better embrace cyber and data security. Another study [16] identified that perception is a major factor which has become engrained in the small business culture to prevent a rm fully understanding the risks and costly mistakes made by uninformed employees. It also highlights the perception of information assurance as a field of concern and concedes that some form of financial assistance and cyber insurance products do have some impact. However, it can be argued that this study do not cover national and more widespread impacts to facilitate the culture change needed.

Another factor outlined to try drive more secure behaviours is with the use of industry products. This leads to another assertion around current behaviours within SMEs relating to market failure. It is argued that the market did help drive the development of products such as cyber insurance, but as discussed in [34], less than 2% of all businesses in the U.K. in 2016 had taken up that insurance option due to the complexity of the offerings of insurance companies.

Although SMEs are aware of the law, they disconnect to the reality of the threats, how relevant they are for their business and, also, cannot justify the effort to reward ratio in implementing a more secure posture. Therefore, it is logical to suggest that without the basics such as enforceable legislative or financial drivers in place, there is an apathy shown towards standards and investments into cybersecurity by smaller businesses when cost control is such a major challenge. There are several factors that need to be analysed to understand the behaviours of SMEs around cyber or information security. [5] suggests the focus of research has been too centred around a single behavioural trait; namely policy compliance. This is further narrowed as the outcome variable is set to the 'intention to comply with the information security policy'. This approach lacks several other factors such as organisational security maturity and legislative obligations and the questionable perception that SMEs fully understand the legal implications or requirements.

2.2 Attitudes and awareness to cyber or information security standards

[18] suggests that smaller companies would not undertake the larger establish standards such as ISO 27001. And it indicated attitudes and awareness related challenges including lack of internal expertise or understanding the risks of not having such a system in place; the cost to implement and manage the standard; the complexity of implementing the standard; SMEs perceived ISO27001 suitable for only larger organisations. Similarly, [1] suggests that, "...cost and lack

of awareness of the standard contents act as a main barrier for adopting the standard ISO 27001". [18] was written only a year after the scheme had been officially released. However, the follow-up paper [19] was two years after Cyber Essentials had been released, but this still showed a low take up of the scheme. It showed that out of a total of 1688 Cyber Essentials and CE Plus certifications, 540, 777, 352 and 19 certificates were issued by CREST, IASME, QMGS and APMG certification bodies, respectively.

A recent survey [33] highlights that overall only 9% of UK businesses were aware of the Cyber Essentials scheme. This percentage increased in another survey [32] which showed 21% of UK businesses were aware of Information Security Management 27001. It disclosed that around 70% of U.K. SMEs are not aware of the recognised certifications in cyber or information security.

2.3 Comparable behaviours and approaches from other industries

This section looks at other industries that have implemented assurance schemes and how they have successfully influenced behaviours within SMEs. A comparable area that has come from reviewing related work shows the areas of health and environmental activities as one to further investigate [3]. One example is [6] who argues that health psychology has connected relevance to cybersecurity psychology as health behaviours are similarly sensitive to that of information security.

In the U.K., the Food Standards Agency has successfully implemented a local authority mandated scheme called the Food Hygiene Rating Scheme (FHRS) [14]. The FHRS rating system is measured on the standards of food hygiene found at a business following an inspection. This then allows consumers to make an informed decision on whether to eat at that business based on the assessed hygiene standards, measured from 1 worst to 5 the best. This mandated scheme has proved to be a driver to encourage businesses not performing well to do better and those that are achieving high scores, to use that as a marketing tool to attract customers. Consumers are used to seeing number ratings or star-based scores for areas like hotel ratings, business reviews, and food hygiene as they provide an instant and understandable reference point to help enable a consumers buying decision. When looking at how to drive-up standards in SMEs, FHRS provides additional insight as reported by BBC News [4], who showed a significant rise in Welsh businesses aiming and achieving the top 5 rating, which was up from 45% to just under 61% in 2015. It also reported that the "ratio of firms rated satisfactory or better (scores 3 to 5) rose from 86.9% to 94.4%, while the number of outlets with a zero-rating halved from 134 to 61, around one in 500".

Treating cybersecurity like the Government treats infectious diseases is a must, and it is widely accepted that individuals are responsible to make life choices to improve their own well-being, though we also often engage in some degree of risky behavior [28]. FHRS aims to reduce the incidence of food borne illness and the associated costs to the economy. A similar objective can be argued for cybersecurity, where the aim is to reduce the incidences of data breaches and cybercrimes and the associated costs and disruption to the economy, business,

and the public. Hence, the need of aligning the merits of cybersecurity with an established scheme such as FHRS.

2.4 Information availability and its dispersion to SMEs

A key challenge identified was around how SMEs find security-related information and the impact the dispersion of information has had on the SMEs security posture [34, 35, 2]. These studies highlight the confusing landscape that the vast array of online channels offer when searching for information. The key question is how to deliver consistency as the content is not regulated? It is not clear how an SME would judge whether the source is trustworthy, or that the guidance given is relevant for them. SMEs are confused about what information to go with due to the sheer volume of available data and, often, do not know where to begin. The study [34] showed that only 7% of businesses consulted government websites and the Government's survey showed only 2%. It argues that for the sake of publicity, concerned news or media reports tend to focus on high-profile data breach cases even if similar attacks happen against SMEs. That may lead to the misguided assumption that SMEs are not at risk. Hence, the Government's attempts at priming or a warning SMEs do not influence the degree of information disclosure [22].

The European Union Agency for Network and Information Security (ENISA) organisation did provide a contribution in this topic around an effective way to share information through the utilisation of the U.K.'s Cybersecurity Information Sharing Partnership (CISP)[12] . This would position CISP as a trusted exchange partner for business to seek guidance on cyber threats and data security issues. ENISA [12] does state, "Such an initiative requires high levels of trust that maybe difficult to achieve amongst large groups of participants". That seems to be a fair assessment of SMEs sharing their information, which raises the question as to whether using anything associated to the Government would be deemed suspicious by SMEs as trust in the U.K. Government has broadly remained unchanged since 2017 at 36% [11].

2.5 Drivers to help deliver increases in positive security behaviours

[30] suggests that management can increase compliance in the domain of information security, by using the social bond theory and the involvement theory as encourages sharing of knowledge and collaboration. Several useful areas were rationalised around how to engage and develop behavioural changes more effectively[5]. One area put forward was the use of vignettes to highlight behaviours as it helps remove the need to admit to personal information but still gain insight into the person's behavioural traits. In addition, individuals are influenced by subconscious cues and this "priming" through visualisation is an important element needed for behavioural change. A further driver raised for consideration is around incentivisation the U.K. government introduced a now defunct scheme of 5,000 innovation vouchers for SMEs back in 2013 [15]. These vouchers could be used to improve information security aspects but even though the actual number

of vouchers taken up is unclear, the take up was at a level the government saw as not being effective. Therefore, three years later from its introduction they were ceased. This outcome partly supports that market failure is a major factor in the low adoption of standards. The five drivers were compliance with laws and regulations, protection of brand and reputation, physical cost of a breach, market pressure for a recognised standard, and stock market price [25, 18].

Several barriers can be extrapolated from the literature that the U.K. SMEs need to face when trying to achieve positive cybersecurity postures [27, 7, 2, 23]. These barriers include: lack of time or financial resource; lack of understanding the risks or threats; lack of incentives to undertake standards or change behaviours; lack of pressure for cyber security within their supply chain or via consumers; lack of compliance drivers; lack of trust in experts or quality of information (including a single source); lack of expertise within the business; and unclear or confusing legislation requirements. These studies also highlight potential opportunities to overcome these barriers that include: protecting cashflow; focusing IT expenditure to deliver the most impact and best ROI; cleansing customer databases for higher engagement and response rates; reducing applicable costs such as cyber insurance or IT financing; better understanding the risks and potential threats for the business; opening new market or business opportunities to support business growth; and developing a competitive advantage. Although any SME will have different weighting ratios of importance against their identified risk factors, the following key research gaps were identified in achieving positive cybersecurity postures for the UK SMEs:

- The perceived benefits for implementing security standards are outlined. But these benefits did not appear to be a compelling solution to help encourage and facilitate U.K. SMEs to take up those standards outside of it being a requirement for a public sector contract.
- Behavioural models are discussed, but a clearly defined incentive-based model that understands the motivational influences for U.K. SMEs to engage in more secure behaviours was missing.
- Several points are raised around needing a nationally mandated model but seemed to just use existing standards even though the market had shown a relatively low take up to date. Therefore, a foundational solution is required that could be mandated, but it must also demonstrate a relevant value proposition to an SME to be deemed as highly advantageous.
- Further work is needed to ascertain how cybersecurity information is obtained and the perceived complexity of it, including the potential impact. The literature also suggest a gap of a single-source trusted information point that is not government controlled.
- There was a lack of a solution that could address informed decision making by consumers around cyber or data security, which also could be used by industry as a benchmark.
- Comparable behaviours in other industries are discussed, but no actual solution is suggested to make effective use of that behavioural approach.

These identified gaps also facilitate the identification of the external and internal influencing factors and their likely collective outcomes when looking at safer behaviours and developing a more secure organisational culture. Since the current standards do not capture and help form the behavioural basis, it has provided the necessary insights to develop a new model.

3 Proposed Rating system

This section presents the proposed cyber rating scheme.

3.1 System evaluation method

The literature highlights limitations of the current cybersecurity standards such as theory choices to influence positive security behaviours, encouraging factors for standards adoption, ineffectiveness of standards, approach aligned with a comparable industry and standards, perceptions and awareness of SMEs. After analysing these limitations, we defined six hypotheses (H) to influence and refine the development of the new cybersecurity-based rating scheme for SMEs:

H1 Incentive theories will influence security behaviours more effectively compared to rational choice theories.
H2 Widespread adoption of a cybersecurity standard requires mandated local authority compliance.
H3 Cybersecurity needs to be more aligned with environmental health in its appreciation and delivery process.
H4 Businesses lack awareness and perception of relevance or value with current cybersecurity standards.
H5 Perceived complexity in cybersecurity perpetuates inactivity and a higher risk acceptance due to the scale of the issue and the diversity of information available.
H6 Giving people rational security information does not guarantee positive behaviour change.

Below are the evaluation methods defined to test the validity of the six noted hypotheses (Section 3.1) and the feasibility of a new scheme:

- Quantitative and qualitative surveys - To provide a data collection method from a question set around technical and behavioural concerns associated with cyber and data security. Also, to gather feedback and positions from areas SMEs experienced or perceived.
- Expert interviews - Through unstructured interviews with industry and academic experts generate qualitative data and gain a deeper understanding of their views and their expert feedback against the submitted hypotheses

3.2 Proposed rating methods

The relatively low take up of existing standards, primarily focus on technical and management systems when undertaking audits. It is also true to highlight the growing threats to SMEs [24], yet there still is a lack of awareness or even

Table 1. Mapping the new scheme sections to the five sections in Cyber Essentials.

Sr. No	New Scheme Technical Sections	Cyber Essential Control Sections
1	Protecting Your Network	Firewalls and Internet Gateways
2	Ensuring Your Systems Are Securely Configured	Secure Configuration
3	Controlling Who Accesses Your Systems	Access Control
4	Protecting Against Malware	Malware Protection
5	Keeping Your Systems Up-To-Date	Patch Management

the implementation of security measures. As only 49% of businesses not having implemented the government's five basic technical controls from Cyber Essentials; hence, this approach is not working [13]. **H6** states providing information, regardless of how rational the arguments, is not enough to positively change behaviours. It also supports the view that rational choice theories are not enough to bring the change; there may be an opportunity for a better incentivised approach to deliver success (**H1**).

A key part of the proposed approach is in the measuring of an SMEs security posture and being able to generate a single-digit (1 to 5) rating to illustrate the cyber competence and data security effectiveness of that business. To achieve this rating, the paper proposes utilising two distinct audit areas to generate a composite rating. The two proposed areas are the SME's security behaviours and their technical systems. The aim being to understand both the technical systems in place to provide mitigation against the various cyber threats as well as understand and, where needed, influence the SMEs behaviours in how those systems are utilised, managed and improved.

One half of the rating function will focus on the technical aspects and for ease of progression will be aligned with Cyber Essentials. The technical audit will cover five sections similar to Cyber Essentials, with Table 1 illustrating how the new scheme's technical audit sections would map across to Cyber Essential's current five sections. The other half of the rating function focuses on behaviours and risk propensity of an SME. From the literature review and industry analysis (i.e., expert reviews as described in Section 4.2), the first iteration of a new quadrant behavioural model has been developed to illustrate what influences may affect an SME's security posture and then allow for levels of weighting to be applied depending on the ratings scored during the audit process.

Fig. 1 shows the assembled behavioural influencing model, named the 'Fan of Influence', and the four distinct segments derived from it are: Fig. 1 shows the assembled new model, named the 'Fan of Influence', derived from the combined analysis of peer research, internal testing, and expert interviews. The four distinct segments deriving from Fig.1 include:

(a) Perception and Understanding [P&U] segment relates to decision influencing coming from how the respondent views and perceives the relevance, threat, risk, and trust of information available. It also covers awareness and how the respondent views the effort to reward ratio.
(b) External (Personal) [EXT (P)] segment relates to external decision influencing coming from within the respondent(s) peer (social or work) network and from past experiences.

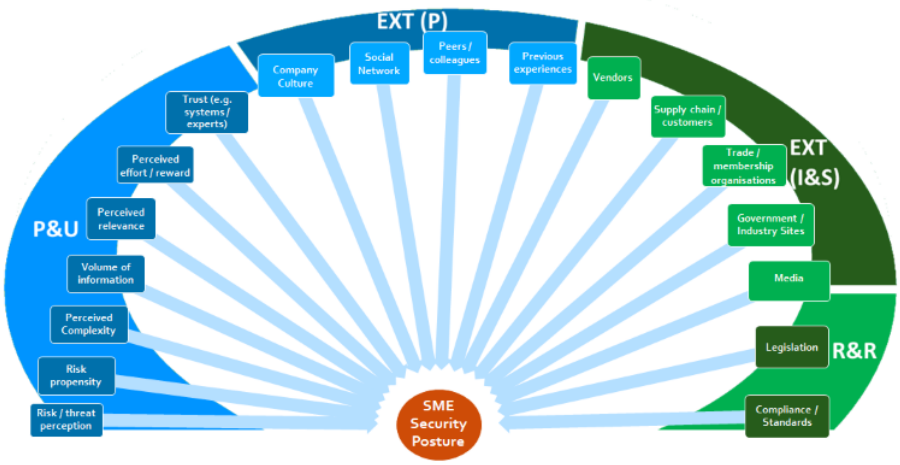

Fig. 1. Proposed behavioural influencing model for an SME's security posture.

(c) External (Inform and Service) [EXT (I&S)] segment relates to external decision influencing coming from entities or organisations that the respondent may interface with during normal business operations. This could be areas which have a greater influence on the respondent(s) business operations such as the supply chain or the vendors they use.
(d) Regulation and Requirements [R&R] segment relates to fixed decision making which are typically a requirement (be it legally or as a standard) which the respondent must follow. There is usually little to no influence the business themselves could have on these factors.

This behavioural influencing model concept allows each of the four segments (and/or segment piece) to be weighted depending on the business and the threat requirements generated through dynamic means, such as intelligence-based decision making [10]. The ability for this model to incorporate individualistic influencing factors and recognise the context of an SME's security decision making, helps improve the opportunity of better SME engagement. It also develops positive security behavioural change through SME owners understanding the relevant value proposition to their business and the potential benefits of implementing such measures aligned to the current and changing threat landscape. This level of granularity and behavioural analysis provides a distinctly different approach to existing security standards. It is envisaged that the proposed behavioural model would utilise a top-to-bottom approach when dealing with cybersecurity improvements and issues as SMEs are typically owner-led which is the vital source for delivering an organisation-wide culture of security. The challenges to information security best practices and corporate culture come from at least three factors: level of threat perceived, location, and lack of cooperation and communication between management and staff. Recent research has shown

that positive information security culture encourages security-vigilant behaviour of employees and therefore can help to avoid human-related security breaches [7].

3.3 Defining the rating matrices

The proposed scheme would use a composite rating based upon two layers of assessments; namely the behavioural and technical audit scores. The result will deliver a single-digit score aiming to be easily understood by consumers and businesses alike.

In terms of the scoring matrices themselves, we propose the use of a recognised 5x5 approach [29, 31]. Typically, the size of a matrix tends to be a personal choice and aligned to many aspects, such as what is used by the industry? or what customers require to use? The 5x5 size of the chosen matrices will provide enough granularity when defining priorities for secure behaviours and identifying consequences of threats and maps well for the proposed composite rating and its associated thresholds needed to define a single-digit visible rating. This size of matrix is also compatible with the recognised standards of Cyber Essentials, ISO 27001/05, and IEC 31010.

The first layer required to generate the composite rating is based on results from the audit around an SME's behaviours and risk propensity. This scoring focusses on aspects of insecure behaviours which would impact on the business and its customers. It is envisaged that the first layer of scoring (see Fig. 2) measures the likelihood of insecure behaviours against the consequences to the business, with the highest score demonstrating the most insecure behaviour posture. This rating will be used with the technical audit score to produce the nal composite score.

To deliver an actionable plan from the first layer findings, an additional phase within the behaviour layer is required. This phase will utilise the behavioural models outlined in Section 3.2 to identify priorities which have the maximum opportunity to inuence secure behavioural change in that SME. This phase scoring is based on the premise that just identifying insecure behaviours is not enough and identification of actions is also required. Regular undertaking of this approach will ensure continual improvement as it will assist with the denition of priorities through the individually identified influencing factors for each business and ensure costs and outcomes are aligned to that business' objectives. Any identified action implemented or not could then influence the scoring following a review of the first phase. Both Fig. 2 and Fig. 3 use the proposed scoring matrix dimension, and each provides a key as to how the numbers are interpreted in terms of priorities for action or in measuring the impact of insecure behaviours. The score from Fig. 3 is not currently used in the composite score as it is designed to be remedial only.

The second layer to be scored is around the technical and systems side of a business. For this, the information is gathered using a modified audit from the Cyber Essentials standard. That then enables the promotion of the five baseline

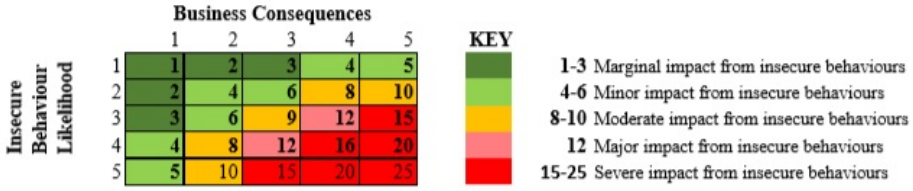

Fig. 2. Phase 1 of behavioural scoring matrix around an SME's security posture.

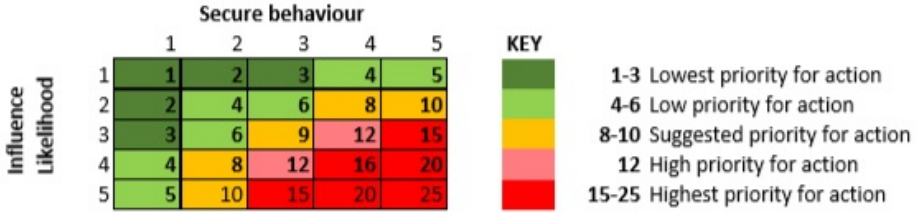

Fig. 3. Phase 2 of behavioural scoring matrix around an SME's security posture.

controls needed for business and streamlines the progression to achieve Cyber Essentials certification. The proposed 5x5 matrix is based on two measures: threat likelihood and business consequences. Much like a traditional risk assessment of impact and likelihood, this structure allows for any easier way to understand the risks for a business and therefore, its customers. That is a vital piece of knowledge when looking to design a rational and comprehensive cyber rating. Fig. 4 shows the proposed scoring matrix and provides a key as to how the numbers are interpreted in terms of business consequences. The score generated from this matrix and the summation from the results from Fig. 2 provides the final composite rating (see Section 3.4).

3.4 Composite scoring

A key foundation to the need of this composite rating is that the current standards are lacking understanding of SME's behaviour and risk propensity. Part of the implementation of this scheme is to develop fresh approaches which achieve perception change around cybersecurity and deliver safer behaviours by understanding and influencing behaviours through personalised motivating factors.

Therefore, to achieve this, the process is to take the results from both matrices shown in Fig. 2 and Fig. 4 and generate the final score from a summation of those two matrices. Fig. 5 shows the thresholds and its associated rating. The threshold can be refined based on further research, but with the use of a 5x5 for the two scoring models it allows for most of the results to fit within 'Satisfactory' ratings and below and provide a higher threshold for 'Good' and 'Excellent' ratings. This is seen as desirable as businesses should be at a high level in both of the audited layers to demonstrate secure behaviours as well as secure systems as a business

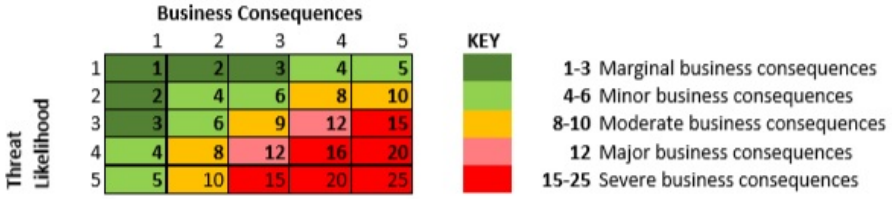

Fig. 4. Proposed 5x5 scoring matrix around an SME's technical risk and threat vulnerability.

KEY	Threshold	Rating Description	Rating	Min %	Max %
	2-17	Excellent	5	80%	100%
	18-24	Good	4	64%	74%
	25-31	Satisfactory	3	50%	62%
	32-37	Above Basic	2	36%	48%
	40-50	Basic	1	4%	34%

Fig. 5. Proposed composite table to derive the new schemes final security rating.

must have at least one '5' rating to achieve a 'Good' or above. It also means businesses have to score at least 50% in total to be deemed 'Satisfactory'. The min and max percentage ranges in Fig. 5 show the range of scores that would be achieved in that rating's banding.

The threshold for the scoring follows the model of the previously discussed FHRS rating in Section 2.3, as that has been a proven model which has been both successfully implemented and managed regionally.

Once a composite rating is calculated from Fig.5, it then leads to the visible rating seen by consumers and businesses. To further align it with successful models, such as FHRS, the proposed scheme will use a simplified and recognised scoring approach of 1 to 5 stars with a simple rating explanation included (columns three and four of Fig.5). A rating of zero is not included as that would mean the business is unrated and failed the audit. This approach is to immediately provide consumers and other businesses the ability to make informed decisions as these ratings would be visually displayed at the entrance, near the payment area and online.

4 Evaluation

This section presents the initial scheme testing and evaluation strategy. Following the defined system evaluation methods (described in Section 3.1), the testing will be done over two distinct methods: (a) quantitative surveys with at least one qualitative question and (b) expert non-structured interviews. These evaluation methods are designed for preliminary evaluation of the scheme, but the results

Table 2. Profiles of experts.

Expert Reference	Background	Expertise and Experience
Expert 1	Academia and research	Noted and published professor in cybersecurity with vast research experience in human-centred security and behaviours towards business (especially SME sizes) and cyber and data security.
Expert 2	Financial and legal industry	Head of innovation within a large, blue-chip service organisation specialising in offering financial and legal products for business. Oversees innovation projects such as one with machine learning based on behaviours.
Expert 3	Local government	Information Governance Manager for a large district council. Oversees multi-agency information sharing to ensure processing is compliant with data protection legislation. Remit also includes awareness of governance and training through the boroughs and local enterprises around many cyber and data centric subjects.
Expert 4	Local government	Information Governance Manager for a city council. Many years of experience in all areas of governance and information assurance, including working with local authority business development teams to help local businesses grow. Also, has long experience with data security regulations and supply chain procurement processes within the local authority.
Expert 5	Banking industry	Lead manager in digital engagement for a major international bank. Their role focuses on businesses with turnovers up to 6 million and is tasked to help provide guidance and raise awareness in cyber and information security. Proven experience in training and event presenting with an expertise in cyber fraud.

do provide evidence around its feasibility and applicability and help form a foundation for further extensive testing and research.

4.1 Surveys

There were two surveys completed: a technical and a behavioural survey with the same 15 respondents and with 10 questions in each questionnaire to collect both quantitative and qualitative data. The sample size is too small to be representative of the SME population. However, the conducted surveys do provide indicative conclusions and useful insights to support the initial evaluation of the new scheme.

The results from the technical controls and systems survey are given below:

- Nearly 9 in 10 businesses (87%) stated they had one or more firewalls protecting their network. However, 54% of those businesses stated that they do not regularly review their firewall rules.
- A third of all surveyed businesses admitted that they do use the same password across multiple accounts, with 80% of all surveyed micro businesses stating that they did this.
- 8 out 10 surveyed businesses stated that they change their passwords every quarter or twice a year, with only around 1 in 10 (13%) stating their change passwords monthly or less.
- 6 out of 10 surveyed businesses stated that they did have a user account creating process, but 80% of micro and 33% of small-sized businesses said they did not.

- The majority (53%) of surveyed businesses indicated that they did not have anti-virus or malware protection for every Internet-enabled device, which included 83% of all small-sized businesses. From those that did have malware protection, businesses regularly scanned for viruses daily/weekly or monthly.
- 60% of all surveyed businesses did state that they ensured at 'most times' they had the latest updates on installed software.
- Over 7 in 10 businesses (73%) stated that they did not perform regular vulnerability scans on their owned networks, with only medium-sized businesses stating that they did.

The results from the behavioural and risk propensity survey are given below:

- A third of surveyed businesses did not consider cyber threats or data loss a significant risk to them.
- Most businesses felt that GDPR was relevant to their business (60% stated fairly or very relevant responses). However, most businesses (80%) found the new data protection regulations fairly or very difficult to understand.
- Almost equal amount of businesses was aware of Cyber Essentials and ISO 27001 (53% to 47% were not aware of them) with 100% of Accommodation and food services businesses and 66% of Professional, scientific, and technical businesses not being aware of Cyber Essentials.
- The majority of businesses (66%), especially the Education businesses surveyed, would speak to friends or colleagues when wanting help on a cybersecurity issue.
- Most businesses (73%) found understanding information on cybersecurity to be either fairly or very difficult to understand, especially from the small-sized businesses surveyed.
- A third of businesses felt like there was not enough information about cybersecurity available to them, but 40% of businesses stated that there was either slightly too much or overall, too much information available.
- Trust in the information available was reasonable with 47% trusting most of the information with 53% trusting some of it.
- The most stated theme when looking at what cybersecurity areas the surveyed businesses needed help with was around compliance and auditing. The two main technical responses were around network security & threat analysis and incident handling. The other key theme raised was around better training, guidance and awareness.

4.2 Expert interviews

The experts selected for unstructured interviews fitted across the following three profiles: commercial or industry, academia, and local government. These profiles helped to give a broad understanding of the various aspects associated with the proposed scheme. Table 2 lists the profiles of the five experts engaged with for this paper.

During expert interviews, the initial discussions were on the expert's experience and thoughts around a new foundational scheme in cybersecurity for SMEs.

Table 3. Summary of experts supportive of the hypotheses from section 3.1

	Hypotheses	Supported By
H1	Incentive theories will influence security behaviours more effectively compared to rational choice theories.	Experts 1, 2.
H2	Widespread adoption of a cyber security standard requires mandated local authority compliance.	Experts 3, 4.
H3	Cybersecurity needs to be more aligned with environmental health in its appreciation and delivery to business.	Experts 2.
H4	Businesses lack awareness and perception of relevance or value with current cyber security standards.	Experts 1, 2, 3, 4, 5.
H5	Perceived complexity in cyber security perpetuates inactivity and a higher risk acceptance due to the scale of the issue and the diversity of information available.	Experts 2, 3, 4, 5.
H6	Giving people rational security information does not guarantee positive behaviour change.	Experts 1, 2, 5.

In addition, the six hypotheses from Section 3.2 were discussed. Table 3 lists the six hypotheses and, the experts who supported each of these statements.

5 Conclusion and Future work

To sum up, there is a perception of complexity around cyber and data security, especially with the new data protection regulations, and a big area that is needed is behavioural change. The U.K. Government wants more SMEs involved in their supply chain but there is little evidence to suggest that there will be enough secure and well managed SMEs in terms of cybersecurity that could help achieve that aim. To that extent, the movement away from purely rational choice-based theories and information dispersion needs to be looked in-depth as this paper has suggested. The proposed system helps gain a personalised understanding of the risk propensity and influences on secure behaviours for each business, rather than just what secure technical systems and policies are in place. Further work is needed to generate larger levels of evidence, but it demonstrated there are core reasons around why SMEs are not embracing the merits of robust cybersecurity standards and best-practices more widely, such as Cyber Essentials which was specifically developed to engage U.K. SMEs, Awareness of such standards and the perceived relevance and risk propensity are major factors for the current market failures. To make this scheme a success, these factors would need to be addressed. This could be achieved by following the FHRS model of enforcing such a programme at regional level through local government authorities mandating any businesses handling personal data as an example and then the composite approach involving understanding and measuring behaviours and influencing factors to ensure that SMEs are engaged through relevant, personalised measurements and actionable plans which generate value-based outcomes and develop positive security behavioural change. The immediate future work includes:

– Undertake larger survey base to test and refine the two-layer audit model for robust testing of the 'Fan of Influence' model and the six hypotheses. Develop

the required audits against the two-layered scoring models and then map the answers to suitable scoring within the matrices.
- Develop a new model for the weighting ratio required for the proposed scheme as a 50/50 ratio would not be reflective of industry needs. The new weighting model could utilise intelligence-based decision making from data generated by accredited national security surveys and other such industry accepted sources. Attack types could then be sub-divided into behavioural-based (or the human error factor) and technically-based to facilitate a dynamic annual weighting to be applied to the composite rating process which would focus the weighting ratio on the current threat landscape each year and not rely on the knowledge of the persons undertaking their risk assessments within the current security frameworks.
- Further develop the incentivised benefits and drivers, including investigating a mandated supply chain process which could be mirrored within the public sector at a regional level.
- Extend the mapping exercises of the new scheme against ISO 27001 and Cyber Essentials to see what percentage of each standard have been undertaken and, therefore, provide a visual guidance to a business in how much more work is required to meet other standards to further encourage take-up.
- Include analysis on other non-U.K. standards, such as NIST-800 and the Cybersecurity Framework to identify if anything of value could be learned which helps facilitate this model being utilised in other countries.
- Carry out a detailed quantitative pilot study within chosen regional locations and with approximately 20-30 active business. Using sectors, such as retail, would provide responses from both consumers and businesses on their perceptions of the new scheme and, having a visible cybersecurity rating may allow for measurements in areas like commercial advantage and consumer confidence which help develop the value proposition of the scheme.

References

1. Alqatawna, J.: The challenge of implementing information security standards in small and medium e-business enterprises. Journal of Software Engineering and Applications **7**(10), 883–890 (2014)
2. Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672 (2019)
3. Barton, K.A., et al.: Information system security commitment: A study of external influences on senior management. Computers & Security **59**, 9–25 (2016)
4. BBC News: Food hygiene ratings scheme in wales 'a big success' (2015), https://www.bbc.co.uk/news/uk-wales-politics-34943449
5. Blythe, J.: Cyber security in the workplace: Understanding and promoting behaviour change. Procs. of CHItaly Doctoral Consortium **1065**, 92–101 (2013)
6. Blythe, J.M., Coventry, L., Little, L.: Unpacking security policy compliance: The motivators and barriers of employees security behaviors. In: Eleventh Symposium On Usable Privacy and Security. pp. 103–122 (2015)
7. Connolly, L., Lang, M.: Information systems security: The role of cultural aspects in organizational settings. Information Systems Security (2013)

8. Crown Commercial Service - GOV.UK: The sme spend target must go on (2018), https://www.gov.uk/government/news/the-sme-spend-target-must-go-on
9. Cyberaware.gov.uk: Small business reputation and the cyber risk- cyber streetwise and kpmg. Tech. rep., Cyber Streetwise and KPMG (2015)
10. Dilek, S., Çakır, H., Aydın, M.: Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552 (2015)
11. Edelman: Trust barometer 2018 - uk findings (2018), https://www.edelman.co.uk/magazine/posts/edelman-trust-barometer-2018/
12. ENISA: Cyber security information sharing: An overview of regulatory and non-regulatory approaches (2015), https://www.enisa.europa.eu/
13. Finnerty, K., et al.: Cyber security breaches survey 2018 (2018), https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018
14. Food Standards Agency - FHRS: Food hygiene rating scheme (2019), https://www.food.gov.uk/safety-hygiene/food-hygiene-rating-scheme
15. Gov.uk: Innovate uk widens the appeal of 5,000 vouchers for small firms to seek expert advice. (2014), https://www.gov.uk/government/news/innovation-vouchers-for-all
16. Gundu, T., Flowerday, S.: Ignorance to awareness: Towards an information security awareness process. SAIEE Africa Research Journal **104**(2), 69–79 (2013)
17. Hancock, M.: Cyber security speech at the institute of directors conference (March 2017), https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference
18. Henson, R., Garfield, J.: What attitude changes are needed to cause smes to take a strategic approach to information security? Athens Journal of Business and Economics **2**(3), 303–318 (2016)
19. Henson, R., Garfield, J.: Smes attitudes to information assurance and consequences for the digital single market. In: Athens: ATINER'S Conference Paper Series, No: SME2016-2278. pp. 1–19. Athens Institute for Education and Research (2017)
20. ICO: Guide to the general data protection regulation (gdpr) (April 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
21. ISO: Iso /iec 27000 family (April 2019), https://www.iso.org/isoiec-27001-information-security.html
22. Junger, M., Montoya, L., Overink, F.J.: Priming and warnings are not effective to prevent social engineering attacks. Computers in human behavior **66**, 75–87 (2017)
23. Kabanda, S., Tanner, M., Kent, C.: Exploring sme cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce **28**(3), 269–282 (2018)
24. Kurpjuhn, T.: The sme security challenge. Computer Fraud & Security **2015**(3), 5–7 (2015)
25. McIlwraith, A.: Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge (2016)
26. NCSC (National Cyber Security Centre): Cyber essentials: The sme spend target must go on (April 2019), https://www.cyberessentials.ncsc.gov.uk/
27. Osborn, E., Simpson, A.: On small-scale it users' system architectures and cyber security: A uk case study. Computers & Security **70**, 27–50 (2017)
28. Renaud, K., et al.: Is the responsibilization of the cyber security risk reasonable and judicious? Computers & Security **78**, 198–211 (2018)
29. Ristić, D.: A tool for risk assessment. safety Engineering **3**(7), 2017 (2013)
30. Safa, N.S., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Computers & Security **56**, 70–82 (2016)

31. Shuttle, M.: Project risk manager: Risk matrix sizing: Does size really matter? (2017), https://www.project-risk-manager.com/blog/risk-matrix-sizing/
32. Statista: U.k. businesses awareness of iso 27001 in 2017 (2017), https://www.statista.com/statistics/586556/iso-27001-awareness-by-united-kingdom-uk-businesses/
33. Statista: U.k. businesses that are aware of the cyber essentials scheme in 2018 (2018), https://www.statista.com/statistics/586565/cyber-essentials-scheme-awareness-by-united-kingdom-uk-businesses/
34. Topping, C.: The role of awareness in adoption of government cyber security initiatives: A study of smes in the uk (2017)
35. Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems **24**(1), 38–58 (2015)